

Patent Claims

ART 34 AMDT

1. A method for protected execution of a cryptographic calculation,
in which a key (12) with at least two key parameters (p, q, pinv, sp,
5 dp, sq, dq) is drawn on, wherein an integrity check (30, 34, 40, 54)
of the key (12) is performed in the method, in order to prevent a
cryptographic attack in which conclusions are drawn as to at least
one second key parameter (p, q, pinv, sp, dp, sq, dq) by corrupting
at least one first key parameter (p, q, pinv, sp, dp, sq, dq),
10 characterized in that at least one key parameter (dp, dq) is the
product of a value required for the cryptographic calculation times
a safeguard value (sp, sq), and in that the integrity check (30, 34,
40, 54) includes a divisibility check.
- 15 2. A method as claimed in claim 1, characterized in that the
safeguard value (sp, sq) is contained in the key (12) as a key
parameter.
- 20 3. A method as claimed in claim 1 or claim 2, characterized in that the
cryptographic calculation is an RSA-CRT method, and in that the
value required for the cryptographic calculation is a CRT
exponent, wherein the product of this CRT exponent times the
safeguard value (sp, sq) is contained in the key (12) as a
safeguarded CRT exponent (dp, dq).
25
4. A method as claimed in one of claims 1 to 3, characterized in that
in the integrity check (30, 34, 40, 54) it is checked whether a key
parameter (p, q, pinv, sp, dp, sq, dq) or a value which differs from
the key parameter (p, q, pinv, sp, dp, sq, dq) by a multiple of the
30 safeguard value (sp, sq) is evenly divisible by the safeguard value
(sp, sq).

ART 34 AMDT.

5. A method as claimed in one of claims 1 to 4, characterized in that in the integrity check a checksum stored with the key parameters (p, q, pinv, sp, dp, sq, dq) is compared with a checksum newly calculated after passing of the key parameters (p, q, pinv, sp, dp, sq, dq).
5
6. A method as claimed in one of claims 1 to 5, characterized in that, to check the integrity, important parameters to be passed are multiply passed and checked for identity after passing.
10
7. A method as claimed in one of claims 1 to 6, characterized in that the cryptographic calculation is a decryption or signature generation according to an RSA method, in particular an RSA-CRT method.
15
8. A method as claimed in claim 7, characterized in that in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check (30, 34, 40, 54) it is checked whether the exponent used in the exponentiation operation results as an integer quotient of a division of a value by a safeguard value (sp, sq).
20
9. A method as claimed in claim 8, characterized in that in the cryptographic calculation an exponent blinding method is applied for protection against spying.
25
10. A method as claimed in one of claims 7 to 9, characterized in that the prime factors (p, q) of the RSA method are multiplied by a masking parameter (j) and the error freedom of the calculation
30

sequence is checked by an equality check modulo the masking
parameter (j).

- 5 11. A method for determining a key for a cryptographic calculation
 with at least two key parameters (p, q, pinv, sp, dp, sq, dq),
 wherein the key is provided for use in a method as claimed in one
 of claims 1 to 10.
- 10 12. A computer program product which has program commands to
 cause a processor to execute a method with the features of one of
 claims 1 to 11.
- 15 13. A portable data carrier, in particular a smart card or chip module,
 set up for executing a method with the features of one of claims 1
 to 11.